

The Ohio Department of Higher Education Articulation and Transfer Clearinghouse (ATC)

DATA ACCESS AND SECURITY POLICY Established September 13, 2007

Section 1: Purpose

The Articulation and Transfer Clearinghouse is a software system developed and operated by the ODHE for the purpose of routing electronic transcripts for the Ohio state-assisted colleges and universities. Additionally, the ATC matches courses taken by a student at his or her current institution with courses reviewed and approved to be “equivalent” under the State’s Articulation and Transfer Policy. These equivalencies are documented in a transcript supplement but not in the original transcript. This document outlines the policies and procedures that are in place at the Ohio Department of Higher Education (ODHE) to ensure the security and privacy of ATC data.

ATC staff will monitor these policies and communicate changes as events or technology warrant. Please contact Revathi Kumaraswamy (rkumaraswamy@highered.ohio.gov) at the ODHE for questions.

Section 2: Definitions

- A. Confidentiality means how personally identifiable information collected by an authorized agency is protected and when consent by the individual is required.
- B. Education records means those records directly related to a student and maintained by an educational agency or institution.
- C. Family Educational Rights and Privacy Act or FERPA means the federal law codified at 20 U.S.C. 1232g and its implementing regulations found in Title 34 C.F.R. Part 99. A description and additional information can be found at: <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- D. Legitimate educational interest, for purposes of this policy, is an endeavor that furthers the understanding of educational practices, methods, and/or theory through formal, accepted research practice.
- E. Personally identifiable information means information contained in an education record such as a personal identifier, characteristic, or other information that would make a student’s identity easily traceable.
- F. Privacy means the right of an individual to have personal information adequately protected to avoid the potential for substantial harm, embarrassment, inconvenience, or unfairness.
- G. Research means a formal investigation designed to develop or contribute to general knowledge.

- H. Two courses or combinations of courses are equivalent under the Articulation and Transfer Policy if they have each been approved by a panel of faculty members as meeting the same learning outcomes at the same point in time.
- I. A human user of the ATC is a person with a role that allows the uploading and/or downloading of transcripts and transcript supplements. A system user of the ATC is another computer system with the capability of delivering transcripts to or retrieving transcripts and transcript supplements from the ATC.

Section 3: Data Security

- A. Security includes the measures in place to ensure that records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. Since the data are stored on computers, it is essential that there be a high level of protection that provides integrity and availability commensurate with the level of risk and magnitude of harm.
- B. ATC data are maintained on a secure computer system and archived daily. Archived information is stored in a fire-proof off-site location. The procedures used to ensure the privacy and security of computer records include but are not limited to: password applications that restrict access to data elements and files only to those with authorization, frequent password changes to guard against break-ins, the use of encryption, and monitoring of user access to the secured files.
- C. All external connections to the agency's restricted data are controlled and restricted by a State of Ohio Department of Administrative Services firewall and a secure web server implementing Secure Socket Layer (SSL) technology. Communication with agency servers is encrypted and requires username and password authentication.
- D. The ATC will enforce security of computer systems through appropriate hardware/software, systems, authorizations, and practices required to ensure the confidentiality of computing systems and data. Users must not violate confidentiality of data by sharing files or information with unauthorized individuals or provide access to confidential data to unauthorized individuals.
- E. The Social Security Numbers (SSN's) and Student Identification Numbers (SID's) are the primary unique identifier for student data in the ATC and are collected from Ohio colleges and universities for the evaluation of state assisted programs in accordance with FERPA

Section 4: Data Access

Data in the ATC is not publicly accessible. Additional data are considered by the ODHE to be restricted, and may not be accessed without authorization by

campus liaisons and the ATC Project Manager. The procedures discussed in this section refer to access to “restricted” data.

- A. Campus liaisons authorize user accounts and assign user roles in the ATC. Role-based access allows an authorized user (human or system), with a legitimate educational need to upload transcripts to and retrieve transcripts and transcript supplements from the ATC.. Users can send and retrieve data associated with only those students currently enrolled in or planning to enroll in their institutions ATC data can be considered sensitive. For these reasons, persons authorized to have access to the ATC should be thoroughly familiar with the transcripts and transcript supplements, and their responsibilities regarding data dissemination noted below.
- B. Transcripts and transcript supplements containing personally identifiable student information can only be accessed and retrieved by authorized users at the institution(s) from which the student was enrolled or to which the student has requested his or her transcript be sent. The responsibility regarding privacy and the appropriate use of the ATC data rests with the authorized user and his or her employing institution. An authorized user must adhere to his or her institution’s policy under Family Educational and Rights and Privacy Act of 1974 (FERPA), as well as, any other institutional procedures pertaining to the security and confidentiality of student information.
- C. Security and confidentiality of ATC data is a matter of concern by the ODHE. The ODHE controls access to ATC data areas. A **Request for Access to Restricted Data Authorization Form** must be signed and completed for any campus user (human or system) or ODHE approved user who is to have access to restricted data areas. Specific instructions are located on the authorization form. Each request for access is individually evaluated by the ODHE and it is expected that only those persons identified on request forms will have access to ATC data. Access is issued to a person or computer system. Approval for access will be evaluated based upon a “legitimate educational interest” or demonstrated “need to know” the information as determined by the campus liaison and/or the ODHE. The ODHE reserves the right to deny access to any such application for access to ATC data.

Section 5: Disclosure of Data

- A. In accordance with Family Educational and Rights and Privacy Act of 1974 (FERPA), disclosure of personally identifiable information in the ATC to the public is not allowed without prior written consent of the institution(s) and person(s) involved. In the event that consent is provided, the ODHE will note the names of the parties who received the information and an explanation of the legitimate educational interest under which the information was disclosed.
- B. The ATC only provides aggregate data to the public in published reports or in response to ad-hoc requests. In planning and producing

analyses and tabulations, the general rule is that there should be no cell (or category) published in which there are fewer than five respondents, or in which personal information could be obtained by subtraction or other simple mathematical manipulations. In these cases an asterisk (*) should be inserted in the cell.

- C. Private or confidential data will be released as stated in federal regulation 34 C.F.R. Part 99 to authorized staff of the postsecondary education institutions who have released the data to the ATC and only when the determination has been made that there are legitimate educational interests, under federal regulation 34 C.F.R. Part 99.36(b)(2).
- D. ATC data should be used for evaluative and planning purposes within the ODHE or within an institution, rather than dissemination beyond a campus used as a method to contact students. In such limited cases where ATC data are disseminated to public settings, the ODHE suggest a policy of *responsible data dissemination*. This policy includes:
 - Removal of any personally identifiable information, including aggregate data that may personally identify an individual.
 - Acknowledgement at all times of relevant data anomalies which have been noted by ATC staff and institutions.
 - Appropriate notice to the ODHE and Chief Executive of any affected institutions that ATC data are to be disseminated (or in a less desirable instance have been disseminated) in a public setting with timely opportunity for campus review of such data.
 - Maintenance of any query code (called SQL) used to generate ATC data outputs. This is necessary to allow external verification of the validity of query code in presenting and interpreting findings.
- E. To encourage responsible data dissemination, the ODHE reserve the right to maintain in a publicly accessible location the identification of all individuals authorized to engage in restricted query access. Further, the ODHE reserve the right to maintain an internal logging of queries of ATC data by authorized users.
- F. The ODHE will provide a current web site for any known campus data anomalies that may be retrieved by restricted data queries and reports. Users are responsible for routine reviews of this web site and being aware of data anomalies that may impact analysis of restricted data.
- G. Any data sharing agreements between the ODHE and other agencies or organizations will be established without compromising the confidentiality of individuals. If a data set containing personally identifiable information is released across agencies or to outside organizations the following conditions must be met:

- A written explanation of the legitimate educational interest for data sharing. The data are used solely for the purpose requested
- Appropriate agreements must be signed by all parties to ensure compliance with FERPA
- All records will remain private and destroyed when no longer needed
- The party to whom the data are released does not disclose the information to any third party
- Penalties for inappropriate records use or re-release of records must be stated clearly in the agreement.
- The data are protected in a manner that does not permit the personal identification of an individual.

Section 6: Campus User responsibilities

- A. A person granted ATC access must sign the appropriate **Request for Access to ATC Data Authorization Form** acknowledging an understanding of the person's responsibilities for password security and maintaining the confidentiality of the data that he/she accesses. This signed agreement must be kept on file by the campus liaison and ODHE. For system access to the ATC, the Request for Access to ATC Data Authorization Form must also be completed and signed by both the campus ATC Liason and the campus director of Information Technology.
- B. A person granted ATC access is responsible for security of his/her password and protection of information. At no time should any individual share his/her password with another person, display the password in public view, or install the password for a group account. Each person approved for access is responsible for signing off when finished with access. A system granted ATC access must be secured from unauthorized access and malicious code.
- C. A person granted ATC access must adhere to his or her institution's policy under Family Educational and Rights and Privacy Act of 1974 (FERPA), as well as any other institutional procedures pertaining to the security and confidentiality of student information. In addition, a person with access should be aware that the penalties for violation of FERPA can be the withdrawal of federal funds from the institution, as well as criminal and/or civil sanctions. Similarly, systems granted ATC access must be compliant with FERPA policies and other institutional policies. ATC human users and system users should adhere to local policies associated with handling of transcripts. Furthermore, if an institution has other software applications running on a system with ATC access, it is the insitution's responsibility to verify that the other applications do not interfere with the operation of the interface to or with the ATC itself.
- D. All persons or systems providing or accessing ATC data must guarantee to maintain data about individual students in a secure fashion, such that

- it cannot be viewed by unauthorized individuals by screen, file access, or in printed form. Any personally identifiable confidential data contained in print form or on computer files which are no longer needed should be destroyed in such a way that identification of a student is not possible. **Also see “Section 5: Disclosure of Data” above.** ATC human users and system users should adhere to local policies associated with handling of transcripts.
- E. Users understand that access to the ATC is a privilege not a right and that violations of this policy or its procedures can result in the termination of this privilege and/or disciplinary measures which include legal remedies if required.
 - F. If an employee terminates employment with the institution or transfers within the institution, the Campus Liaison must notify the ODHE in order to initiate access deletion. Computer systems previously authorized for ATC access that are removed from service or reused must have their access privileges removed. A **Request for Access to Restricted Data Authorization Form** must be submitted to the ODHE for such personnel or system replacement.
 - G. If a security violation is detected the human user should immediately change his or her password and notify the Campus Liaison or ATC Help Desk (614-387-0682) if appropriate. If a security violation is detected within a system user, the password should be changed immediately and the Campus Liaison and ATC Help Desk notified. The Campus Liaison is responsible for contacting the ODHE when a password security violation has been detected.
 - H. It is the responsibility of the Campus ATC Liaison and the Campus Director of Information Technology (or equivalent) to demonstrate to the satisfaction of the ATC Project Manager or Institutional Support Person that systems with ATC access are stable, secure and safe from malicious code. This demonstration is required before any system is granted ATC production access and can be performed in the ATC User Acceptance Test environment.

Section 7: ODHE Employee User responsibilities

- A. A person granted restricted access must sign the appropriate **Request for Access to Restricted Data Authorization Form** acknowledging an understanding of the person’s responsibilities for password security and maintaining the confidentiality of the data that he/she accesses. This

signed agreement must be kept on file by the ODHE Supervisor and ATC Project Manager.

- B. A person granted ATC access is responsible for security of his/her password and protection of information. At no time should any individual share his/her password with another person, display the password in public view, or install the password for a group account. Each person approved for access is responsible for signing off when finished with access. A system granted ATC access must be secured from unauthorized access and malicious code.
- C. A person granted ATC access must adhere to the Family Educational and Rights and Privacy Act of 1974 (FERPA), as well as any other agency procedures pertaining to the security and confidentiality of student information. In addition, a person with access should be aware that the penalties for violation of FERPA can be the withdrawal of federal funds from the institution, as well as criminal and/or civil sanctions. Similarly, systems granted ATC access must be compliant with FERPA policies and other agency policies. If an agency system has other software applications running along with ATC access, it is the agency's responsibility to verify that the other applications do not interfere with the operation of the interface to or with the ATC itself.
- D. All persons or systems providing or accessing ATC data must guarantee to maintain data about individual students in a secure fashion, such that it cannot be viewed by unauthorized individuals by screen, file access, or in printed form. Any personally identifiable confidential data contained in print form or on computer files which are no longer needed should be destroyed in such a way that identification of a student is not possible.
Also see "Section 5: Disclosure of Data" above.
- E. A person granted internal ATC access must guarantee to maintain data about the technical infrastructure of the ATC in a secure fashion, such that database, table, and server configurations cannot be viewed by external individuals by screen, file access, or in printed form.
- F. Users understand that access to the ATC is a privilege not a right and that violations of this policy or its procedures can result in the termination of this privilege and/or disciplinary measures which include legal remedies if required.
- G. If an employee terminates employment with ODHE or transfers within the agency where ATC access is no longer part of their duties of employment, the supervisor must notify the ATC Project Manager in order to initiate access deletion. Computer systems previously authorized for ATC access that are removed from service or reused must have their access privileges removed. A **Request for Access to Restricted Data Authorization Form** must be submitted to the ATC Project Manager for any such personnel or system replacement

- H. If a security violation is detected, the human user should immediately change his or her password and notify the ATC Project Manager or ATC ATC Institutional Support Person if appropriate. If a security violation is detected within a system user, the password should be changed immediately and the ATC Project Manager and ATC Institutional Support Person notified.
- I. It is the responsibility of the agency Director of Information Technology (or equivalent) to demonstrate to the satisfaction of the ATC Project Manager or Institutional Support Person that systems with ATC access are stable, secure and safe from malicious code. This demonstration is required before any system is granted ATC production access and can be performed in the ATC User Acceptance Test environment.